REMARKS

Claims 1 - 27 are pending. By this amendment, claims 1 - 16, 21, and 24 are amended. No new matter is introduced. Withdrawal of the rejections and issuance of a Notice of Allowance are respectfully requested.

On page 9 the Office Action notes that claims 10 and 24 contain allowable subject matter.

On page 2 the Office Action objects to claim 24. Claim 24 is amended to overcome this objection.

On pages 2 and 3 the Office Action rejects claims 1 - 27 under 35 U.S.C. § 101. These rejections are respectfully traversed.

Claims 1 - 16 and 21 are amended. Withdrawal of the rejections of claims 1 - 27 under 35 U.S.C. § 101 is respectfully requested.

On pages 3 and 4 the Office Action rejects claims 6, 10, 16 - 20, and 24 under 35 U.S.C. § 112, ¶2. These rejections are respectfully traversed.

Claims 6, 10, 16 and 24 are amended. Withdrawal of the rejections of claims 6, 10, 16 - 20, and 24 under 35 U.S.C. § 112, ¶2 is respectfully requested.

On page 5 the Office Action rejects claims 1 - 6, 14 - 16, 18 - 21, 25, and 26 under 35 U.S.C. § 103(a) over U.S. Patent Publication 2003/0056099 to Asanoma et al. (hereafter Asanoma) in view of U.S. Patent 7,099,476 to Chen et al. (hereafter Chen). This rejection is respectfully traversed.

In rejecting claim 1, the examiner asserts that Asanoma discloses replacing private keys. the Examiner then states that Asanoma "does not explicitly disclose that the rekey request identifies a private key for replacement; however, this feature is deemed to be inherent to Asanoma method because Figures 5 and 9 show that the smart card stores multiple private keys." This statement by the Examiner is totally without any basis, and his conclusion regarding inherency is therefore incorrect. First, Asanoma's smart card is designated by the reference number 30. Figure 5 shows database 14, which most assuredly is not a smart card. In fact, database 14 is shown in general terms in Figure 3 to be part of issue system 23. Smart card 30 is produced by a component of the issue system 23. Figure 9 shows a smart card 30 coupled to user terminal 42. As disclosed starting at paragraph [0071], the smart card 30 is provided to the user with symmetric key Sk. Upon receipt, the user places the smart card 30 into user terminal 42 and "demands" that the issue system 23 generate a key pair and deliver the key pair

(certificate Ct) to the user terminal 42. See paragraph [0075]. The obtained private key RPk then is written to the smart card 30. See paragraph [0076]. to update the private key PRK, this same process is repeated. That is, the smart card 30 is inserted into the user terminal 42, a new public key certificate Ct is sent to the user terminal 42, and the new private key PRk is written to the smart card 30. See paragraphs [0079] - [0081]. This process of updating explains why Figure 9 shows smart card 30 with two private keys PRk. The private keys PRk1 and PRk2 merely represent the original and the updated versions of the private key PRk. Thus, the mere presence of these two keys does not mean what the Examiner states; namely that the smart card 30 stores multiple private keys, and one of those keys must be identified for updating purposes. Instead, Asanoma's system suffers from the same defect as applicants pointed to in the prior art, namely a profusion of private keys that could allow access to restricted information.

Continuing with claim 1, the Examiner notes that Asanoma does not disclose sending a challenge with a rekey request. However, the Examiner asserts that Chen (Figure 2, steps 220 - 250) discloses a challenge, and the further steps of encrypting the challenge with the new/updated key, and returning the encrypted challenge.

Applicants disagree with this characterization of Chen's method. Chen does disclose encrypting the challenge "using the second ciphering key." See column 6, lines 57 - 58. However, in Chen's method, this "second ciphering key" is not provided with the rekey request, nor would such inclusion be inherent or obvious. As Chen makes clear, the "second ciphering key" is provided by access point AP1 after the receiving stations (STA1) and the access point AP1 exchange rekey request and rekey confirmation messages. See column 6, lines 2 - 23. More specifically: "Step 200: after receiving the response to update the ciphering key from the station STA1, the access point AP1 transmits a second ciphering key to update the ciphering key of the station STA1." See column 6, lines 20 - 23. Thus, in Chen's method, the rekey request does not include the "second ciphering key," or, as recited in claim 1, "a SKR key."

In contrast to Asanoma and Chen, claim 1 recites receiving a rekey request, wherein the rekey request includes a SKR key. As noted above, Asanoma and Chen, individually and in combination, do not disclose or suggest this feature. Accordingly, claim 1 is patentable in view of Asanoma and Chen.

The remaining independent claims 16 and 21 recite rekey request features similar to those of claim 1. Accordingly, claims 16 and 21 also are patentable.

Claims 2 - 6, 14 and 15 depend from patentable claim 1; claims 18 - 20 depend from patentable claim 16; and claims 25 and 26 depend from patentable claim 21. For this reason and the additional features they recite, these dependent claims also are patentable.

On page 7 the Office Action rejects claims 7, 8, 17, 22, and 23 under 35 U.S.C. § 103(a) over Asanoma and Chen and further in view of U.S. Patent 6,198,824 to Shambroom. This rejection is respectfully traversed.

Claims 7 and 8 depend from patentable claim 1; claim 17 depends from patentable claim 16; and claims 22 and 23 depend from patentable claim 21. For this reason and the additional features they recite, these dependent claims also are patentable.

On page 8 the Office Action rejects claims 11, 12, and 27 under 35 U.S.C. § 103(a) over Asanoma and Chen and further in view of U.S. Patent 6,886,096 to Appenzeller. This rejection is respectfully traversed.

Claims 11 and 12 depend from patentable claim 1. Claim 27 depends from patentable claim 21. for this reason and the additional features they recite, these dependent claims also are patentable.

On page 9 the Office action rejects claim 13 under 35 U.S.C. § 103(a) over Asanoma and Chen and further in view of Handbook of Applied Cryptology by Menezes et al. This rejection is respectfully traversed.

Claim 13 depends from patentable claim 1, and for this reason and the additional features it recites, claim 13 also is patentable.

In view of the above remarks, Applicants respectfully request withdrawal of the rejections of the claim under 35 U.S.C. § 103(a). Prompt examination and allowance are respectfully requested.

Should the Examiner believe that anything further is desired in order to place the application in even better condition for allowance, the Examiner is invited to contact Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,

Date: **November 6, 2007**

John K. Harrop
Registration No. 41,817
Andrews Kurth LLP
1350 I Street, NW
Suite 1100
Washington, DC 20005
Tel. (202) 662-3050
Fax (202) 662-2739